December 1991/Number 1-92

security awareness bulletin

Inside:

Economic Espionage

Department of Defense Security Institute, Richmond, Virginia

security awareness bulletin

Approved for open publication Unlimited reproduction authorized

Director
Department of Defense Security Institute
R. Everett Gravelle

Editor
Lynn Fischer

The Security Awareness Bulletin is produced by the Department of Defense Security Institute, Richmond, Virginia. Primary distribution is to DoD components and Federal contractors cleared for classified access under the National Industrial Security Program and special access programs. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and education methods.

For new distribution or address changes:

- Air Force: Contact your local Publication Distribution Office.
- Government agencies: DoD Security Institute, Attn: SEAT, 8000 Jefferson Davis Hwy, Richmond, VA 23297-5091, POC Del Carrell, (804) 279-5314/4223, DSN 695-5314/4223; fax (804) 279-6406, DSN 695-6406.
- DIS activities: HQ DIS/V0951, 1340 Braddock Place, Alexandria, VA 22314-1651.
- DoD contractors: Automatic distribution to each cleared facility. Send change of address to your DIS field office.

Intelligence Targeting of U.S. Technology

U.S. Customs Agents Arrest Engineer For Trying To Sell 'Star Wars' Data

Los Angeles Times

Couple Sentenced In Electronics Export Case

Sacramento Bee

As Cold War Fades, Some Nations' Spies Seek Industrial Secrets

Wall Street Journal

KGB Targets U.S. Businessmen, Scientists To Recruit Them As Spies

Washington Times

Gulf War Highlights New Technology Export Control Questions

Defense News

France Spying On U.S. Industry, Using Airline As A Base, NBC Says

Long Beach Press Telegram

Recent headlines in our nation's news media tell it all. The recently proclaimed "new world order" brings with it a radically new perception of the threat. While former adversary nations remain unrelenting in their efforts to obtain critical information by any means, recent events tell us that:

- "The Threat" is actually many threats from many external sources—both governmental and commercial (often working together).

- The highest targeting priority is given to technology (classified or unclassified) which has direct relevance to economic and strategic advantage.

- What is being threatened and who is engaging in collection efforts are determined by specific technological interests; our information may be "targeted" by any country or international organization.

- Members of the scientific and technical community including engineers (both within and outside of government) are increasingly likely to be singled out as espionage targets.

These are the new facts of life around which security professionals must remold their education and awareness activities. In this issue of the *Security Awareness Bulletin*, we offer three selections containing valuable source material for security education. In the first, a very recent assessment of the counterintelligence challenge, FBI Director William S. Sessions identifies new intelligence targets and states that any country can set up an infrastructure to carry out intelligence collection activities in the United States both overtly and clandestinely. These are what Judge Sessions calls "nontraditional intelligence threats" to this country.

One example is the intense activity of the Iraqi intelligence service in the U.S. during the 1980s. A more recent illustration of nontraditional intelligence collection that is currently the subject of press reports, stems from U.S. media interviews with the former chief of the French secret service, Pierre Marion. Marion is reported to confirm that the French have been actively collecting technology and marketing plans from American and other western corporations since the early 1980s. He is quoted by a *Newsweek* report as saying that "It would not be normal that we do spy on these states in political matters or military matters. We are really allied. But in the economic competition, in the technological competition, we are competitors, we are not allied."[1]

It may come as a shock to Americans that some foreign governments do not consider economic espionage for national self-interest to be dirty pool. According to a book by Richard Deacon on the Japanese secret service, "this kind of intelligence work (targeting foreign industry) is regarded as patriotic and just as vital as military intelligence gleaned in time of war." Deacon describes the training of promising young business executives at Japan's Institute for Industrial Protection. This school, established in 1962 to produce intelligence agents for Japanese corporations, includes lessons on telephone tapping and other tradecraft which we normally associate with classic espionage.[2]

Nontraditional espionage is also conducted by traditional adversaries. In this issue of the *Bulletin* we have reprinted the recent intelligence community white paper entitled, *Soviet Intelligence Targeting of the US Scientific Community*. This timely and authoritative document, up to now, has been available to the security community as a separate publication (see our listing of publications in the back of this issue). We believe that this report deserves broader exposure and the immediate attention of security educators in both industry and government. It describes how Soviet intelligence services exploit contact between the US and Soviet scientific communities and focuses on the USSR's efforts to use scientists associated with the Soviet Academy of Scientists to collect western scientific-technical information. Of particular note is a listing of the benefits for specific Soviet military projects from information acquired at seven international conferences. This saved them millions of rubles in long-range research.

Lastly in this issue we have a first hand account of the new global environment in defense industry by William B. Bader.[3] Dr. Bader, who is a senior vice-president at SRI International, describes how major contractors are becoming international in personnel structure and corporate identity. The control and protection of information in this setting becomes a problem of immense proportions that goes far beyond the threat to individual scientists and technical experts. Bader tells us that the protection of certain technologies in the national interest has to do with corporate policy and hard decisions about whether to sell or not to sell a product to a foreign customer. He calls for both better education and better guidance.

[1] *Newsweek*, September 23, 1991, "Parlez-Vous Espionage?"

[2] Deacon Richard: *Kempei Tai, A History of the Japanese Secret Service*, Beaufort Books, New York, 1983.

[3] Reprinted from *Security Awareness in the 90s*, proceedings of a symposium on security awareness held at Monterey Califorina, December 12-14, 1990; Department of Defense Security Institute, Richmond Virginia.

Counterintelligence Challenges in a Changing World

by William S. Sessions

In recent years, the world witnessed some truly amazing events—the fall of the Berlin Wall and the reunification of East and West Germany, the beginnings of democratic governments across Eastern Europe, and the easing of political tensions between the United States and the Soviet Union. As a result, the current perception of most Americans is that foreign intelligence activity directed against the United States and the West is decreasing and, therefore, the need for an active, aggressive counterintelligence response has abated. Unfortunately, this is far from true.

There can be no doubt that important changes are taking place in the world today. However, improved diplomatic relations do not necessarily decrease the foreign intelligence threat to U.S. national security. The truth remains: That threat still exists, as it did in the past and as it will in the future.

Decade of the 1980s

The last decade of the cold war, the 1980s, was designated by the media as "The Decade of the Spy." It was a time when Americans knew who their enemies were—a time when President Ronald Reagan referred to the Soviet Union as "The Evil Empire." The American public showed strong support of counterintelligence efforts and participated in the process by reporting suspicious events.

During the 1980s, more than 45 people were arrested for espionage. Increased human and technical resources, enhanced analytical and training programs, and improved coordination within the U.S. intelligence community and with friendly foreign intelligence services contributed significantly to these arrests. However, much of the success in counterintelligence efforts came as a result of a heightened public awareness of the full damage caused by espionage, as well as the public's support of the measures designed to protect America's vital information.

> **"A heightened awareness by all Americans is the most effective weapon available tomeet the counter-intelligence challenges of today and those of the years to come."**

In addition to the importance of public awareness, the 1980s taught us several other important lessons. First, the American public received a rude awakening regarding the vulnerability of the U.S. national security community from spies within its own ranks. For example, both John Walker and Jerry Whitworth served in the U.S. Navy; Karel Koecher, Larry Chin, and Edward Howard all worked for the Central Intelligence Agency (CIA); Ronald Pelton was a National Security Agency employee; Richard Miller was an FBI Special Agent.

Second, many of the dangers were posed by volunteers. That is, many of those arrested during the 1980s, including Walker, simply offered to spy on their country. And they offered to spy not because they had ideological differences with the U.S. Government or ideological sympathy with a foreign government, as was the case during World War II and the first decade of the Cold War. They spied for the basest of reasons—money.

Third, prosecuting spies was found to be an effective tool to determine the extent of the damage caused to national security. Unfortunately, some of the espionage cases of the 1980s resulted in grave damage to U.S. national security interests. But, without the prosecutions that followed, an accurate accounting of what was lost would not have been possible, and appropriate steps to minimize the damage would not have been taken. Fortunately, in 45 percent of the espionage cases during the 1980s, the work the U.S. counterintelligence community uncovered either prevented the espionage activity or significantly limited the damages.

" ...improved diplomatic relations do not necessarily decrease the foreign intelligence threat to U.S. national security. "

The Changing World

In the 1990s, with the easing of tensions between superpowers and military blocs, it is no longer possible to identify the U.S. counterintelligence mission in terms of these relationships alone—the world has become much too complex for that. America has negotiated historic arms reduction treaties with the Soviets. The Soviets have introduced their programs of Glasnost, openness to the West, and Perestroika, internal economic and political restructuring. And, the world has witnessed the nations of Eastern Europe revolt against their former Communist leaders in favor of new freedom and economic diversity, and in some cases, more democratic forms of government.

While all Americans can agree that the world has changed, and most see that change as positive in terms of an enhanced prospect for world peace, the public tends to view this new world order to be devoid of danger. So, the logic goes, that if there is no longer a threat to U.S. national security, then counterintelligence measures are not needed.

But, the reality is that arms reduction treaties between the United States and the Soviet Union give Soviet "inspectors" potential access to some of this country's most sensitive projects. Glasnost has dramatically expanded the number of exchanges between the United States and the Soviet Union in such areas as business, science, and education. In fact, since Glasnost, the number of Soviets traveling to the United States increased almost 400 percent; in 1990 alone, more than 100,000 Soviets visited the United States. Past experience shows that these exchange groups often contain intelligence officers. Furthermore, the countries of Eastern Europe, while attempting to move away from the Soviet sphere of influence, are now fighting for their own economic survival—and they, too, have a need for Western technology.

Current Intelligence Threats

Arms control treaties between the Soviet Union and the United States will hopefully lead to a diminished threat level between the nations. However, from a counterintelligence perspective, these treaties will give the Soviet intelligence services routine access to sensitive areas and to knowledgeable Americans who are linked to classified information which, until now, was attainable only on a very limited basis. Other treaties currently being negotiated, concerning strategic arms reduction and chemical weapons, would require numerous verification sites, again expanding Soviet access.

But, the Soviets are interested in more than American military secrets. The Soviet economy is in desperate shape and can be revitalized with Western technology, capital, and expertise. In order to strengthen that economy, the chairman of the KGB has publicly stated that it plans to assist Soviet businesses because, as he says, "They are not good businessmen." The Soviets have systematically expanded their intelligence collection beyond military intelligence targets and now routinely include Western economic information and technologies.

Since the Soviet can no longer rely on their former surrogate intelligence services in the Eastern Bloc to collect intelligence for them, they must find other sources of intelligence and develop new surrogate services. The Soviets have started using the intelligence services of other countries to obtain Stealth technology and acquire restricted computer technologies for themselves.

All in all, while the nature of the Soviet intelligence threat may be changing, its objective and actions are not. The Soviet intelligence services are more active now than they have been at any time in the past 10 years, and there is every reason to believe that they will continue their pursuit of Western intelligence during the 1990s.

The threat of Eastern European countries to the United States cannot be fully assessed because they themselves have not yet fully defined the nature and scope of their intelligence services. Some of these countries are no longer collecting intelligence on behalf of the Soviet Union; however, they will, in all likelihood, refocus their collection activities in the United States to fulfill their own requirements. Since, as with the Soviets, the current major focus of these nations is economic reorganization and growth, they also have a real need for Western technology.

What about the People's Republic of China? The PRC has the largest foreign official presence in the United States—2,700 diplomats and commercial officials, 43,000 scholars, 25,000 commercial delegates visiting the United States annually, and 20,000 emigres coming to America each year. The PRC remains a major counterintelligence threat to the United States. Their intelligence services target well-educated Chinese-American scientists and other professionals who have access to useful information and technology using the approach: "Please help China modernize."

While the Soviet Union, the former Eastern Bloc countries, and the People's Republic of China are all traditional intelligence threats, U.S. counterintelligence efforts can no longer focus exclusively on these countries. In this information age, any number of countries can attempt to establish the infrastructure required to carry out intelligence collection activities in the United States, both overtly and clandestinely. Essentially, Americans need to be concerned about nontraditional intelligence threats to this country as well.

With this point in mind, the intelligence activities of countries in the Middle East and Central Asia are becoming more significant. For example, the Iraqi intelligence service was very active in the United States during the 1980s, and in light of the recent war in the Persian Gulf, its activities are likely to continue.

Counterintelligence Responsibilities

The FBI is charged with countering the hostile activities of foreign intelligence services in the United States by identifying and neutralizing these activities. It does this by penetrating these services, disrupting or publicizing their illegal activities, and expelling, arresting, or prosecuting those responsible.

INTELLIGENCE TARGETS

- ECONOMIC
Brokers • Bankers • Finance
- TECHNOLOGY
Business • Institutes • Universities • Laboratories
- AGRICULTURE
Commodity Bankers • Co-ops • Forecasters
- ENERGY
Oil • Gas • Coal • Nuclear • Solar • New Sources
- NATIONAL/INTERNATIONAL AGREEMENTS
Sales and Trade • Exchanges • Cartels

However, the FBI cannot meet its counterintelligence mission alone. Coordination of counterintelligence operations with other members of the intelligence community, and frequently joint operations, is critical to the Bureau's success, along with the support of the Executive and Legislative Branches of the Federal Government, the law enforcement community, and the American public.

While the FBI has the responsibility to make the public more aware of the hostile intelligence threat, it relies heavily on information from the public to fulfill its counterintelligence mission. Because many Americans no longer perceive the Soviet Union and other Eastern European countries as a threat to U.S. security, the FBI must comprehensively expose the full scope of this threat to American institutions, facilities, and citizens. The purpose behind this is to protect national security, not to discourage improved relations and trade between the United States and the rest of the world.

Conclusion

The world is in a constant state of flux. What is true today may not be true tomorrow. For this reason, it is critical to identify the exact nature of any hostile intelligence threat to national security and to counter that threat.

A heightened awareness by all Americans is the most effective weapon available to accomplish this task. By working together, citizens and law enforcement agencies, can successfully meet the counterintelligence challenges of today and those of the years to come.

Reprinted from the Law Enforcement Bulletin, September 1991

One-Liners

For Security Program Promotion

by Joseph A. Grau

During a recent Information Security Management Course, one of the students mentioned an idea to a faculty member. He said he had always found "one-liners" about security—printed in daily bulletins and similar publications—to be a good way of keeping security in people's minds. He also noted that it was hard coming up with fresh ideas for these items time after time. Why couldn't the Institute collect a bunch of these things and publish them for people to use in their security education efforts?

Well, we figured this idea deserved being given a try. On the next two pages are a small collection of security one-liners for you to use as you see fit. How might you use them? Well, maybe you could—

- Print one of them at the bottom of the first page of your organization's daily bulletin, newsletter, or similar publication.
- Use them as slogans on posters—starting points to build posters around.
- Have a poster contest and use one of them as the "assigned topic" for the entries.
- Put them on slides or view-graphs you can use as "fillers" during security education classes, briefings, etc.
- Use one of them as a theme for a "spot" on closed-circuit TV.
- Get other departments (training? safety?) to include one as a leader or trailer on videotapes they produce.

The one-liners in this first set were generated "in-house," and we hope this is the last time we'll be doing that. We know that plenty of you have good ideas you've used (or meant to use) along this line, and we'd like to help you share them. If you have a one-liner (or a bunch of them) you'd like to share, please send them to the Editor of the *Bulletin*. As we get enough together to make up a page-full, we'll share them with our readers. With your help, we hope to make this a regular feature.

Mr. Grau is chief of the Information Security Division, as well as instructor, at the Defense Security Institute in Richmond, Virginia.

Security costs. Good security costs a lot. Poor security costs even more.

If **you** don't care about security, who will?

Good security programs need good people. We need *you.*

Thought about security today?

Poor security + espionage = damage to our national security

THANK YOU for thinking about security.

Security is never the other guy's job!

Information security today = national security tomorrow

Good security makes good sense.

Are you really sure you need all those classified documents?

Who cares about security? We hope *you* do!

A security violation is like a day without sunshine.

Got a question about security? **Ask it!** It may be an important one!

Taking classified work home with you is playing Russian roulette with your career.

Security is part of EVERYONE'S job!

Thinking espionage only happens to the other guy is the surest way to *become* the other guy.

Classified information deserves your protection.

Seen any spies lately? Are you sure?

When's the last time you checked someone's need-to-know?

Life is just a bowl of cherries, but security violations are the pits.

Classified waste contains classified information. Don't forget to protect it!

The only dumb question about security is the one you don't ask.

Security isn't our most important product -- but it's what keeps our products important.

Security is **YOUR** job!

If we forget about security, we might as well forget about our mission.

It only takes one careless person to make a security violation happen.

A lot of people are counting on you to protect classified information.

Soviet Intelligence Targeting of the US Scientific Community

Summary

The KGB and GRU are effectively collecting US scientific and technical information through professional contacts between Soviet and US scientists—these contacts have increased over fourfold since 1984. The Soviet defense industry, a major benefactor, has used such information to advance its technological base in many areas.

Soviet scientists have been tasked as collectors of foreign scientific know-how since at least World War II. During the mid-1960s, however, the program was revamped and expanded, with the scientific community being used as long-term collectors, rather than ad hoc assets. This collection program is controlled by the intelligence services operating within the USSR Academy of Sciences and responds to national-level tasking from the Military Industrial Commission, the powerful overseer of the defense-industrial establishment.

All activities in which Soviet scientists affiliated with the Academy of Sciences might come into contact with their non-Soviet counterparts are filtered through departments attached to the Academy's Presidium that are staffed primarily by KGB and GRU personnel. Those units:

- Evaluate and recruit Soviet scientists into the collection program.
- Expedite travel requests of agents and prospective recruits.
- Give collection guidance and leads—including names of foreign laboratories, companies, and counterparts.
- Furnish funds for entertainment of, and gifts to, counterparts.
- Report on each Soviet scientist's effectiveness as a collector.
- Help arrange scientific conferences and visits to the USSR by foreign scientists.
- Assess and recruit foreign scientists with the assistance of Soviet scientists who participate in the program.

Until recently, almost all Soviet scientists traveling in the West have been associated in some degree with this collection program. A large number of scientists traveling abroad are knowingly affiliated with the intelligence services; they are either working directly for them or are in the process of being recruited by them. Most others not formally affiliated with the intelligence services, nevertheless, have been willing to accept collection requirements. Their motivations in cooperating vary; some do it for financial rewards and personal motivations, such as the expectation of additional travel, advancement, and professional recognition. Some are

driven by the pure pursuit of knowledge; others by patriotism. Only a small number of Soviet scientists have not been involved in the collection program, either because of their academic standing or political connections.

It is not clear how often the Soviet intelligence services attempt to recruit US scientists. What is clear is that Soviet scientists often have been tasked to collect biographic and assessment data on their Western counterparts and to help evaluate their professional capabilities, vulnerabilities, and receptivity to recruitment. If a Western scientist is considered susceptible to an approach, the Soviet scientist can be used to introduce him to a case officer, and in rare cases Soviet scientists reportedly can be used to make the recruitment offer.

The Soviets have become adept at exploiting personal relationships between Soviet scientists and their Western counterparts to acquire classified and proprietary information. They also have been effective in collecting unclassified material that, in aggregate, contributes substantially to the USSR's scientific and technical base.

This collection system appears relatively inexpensive and risk free:

- The host country pays most travel expenses.
- Recruiting, training, and management costs are relatively low.
- The scientist almost always is involved only in legitimate activities that would not stigmatize him as an intelligence collector.

The program helps Soviet scientific knowledge by:

- Immediately helping personal or institute work.
- Responding to national scientific and technical collection requests.

Gorbachev's reforms probably will not diminish the Soviets' desire to use their intelligence apparatus to further their technological capabilities. It is possible that the desire to improve relations with the West and to seek economic assistance may cause the KGB and GRU modus operandi to become more cautious, avoiding high-risk intelligence operations whose exposure would embarrass Gorbachev and tarnish the country's new international image. On the other hand, the country's growing economic distress may make S&T intelligence an even higher collection priority than in the past, so the continued targeting of US scientists seems likely.

Soviet Intelligence Targeting of the US Scientific Community

Introduction

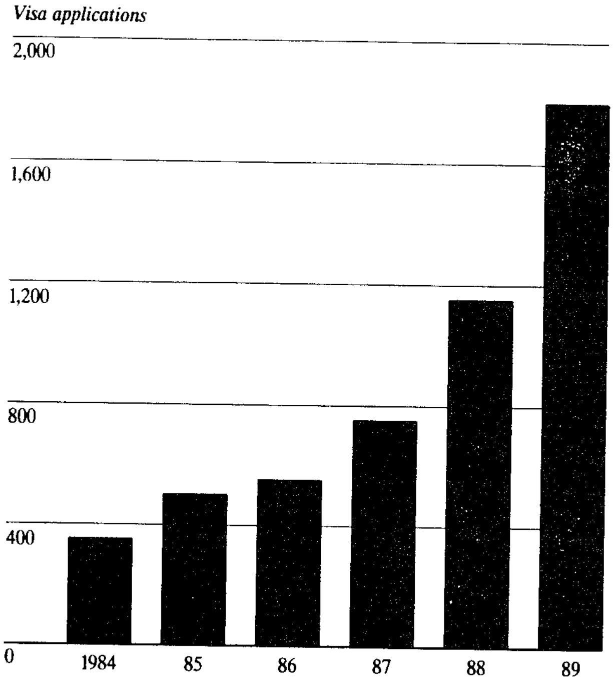
The Soviets are collecting US scientific and technical information by exploiting bilateral professional contacts. Each year Soviet scientists obtain thousands of unclassified and proprietary documents as well as classified data and Western equipment. Virtually every Soviet military research project benefits from these technical documents and hardware, thereby helping the Soviets to advance their technological base.

The importance of this collection technique should increase as official and unofficial contacts continue to expand. We have already seen in recent years a fourfold increase in the number of visa requests for Soviet scientists to travel to the United States—rising from just under 400 trips in 1984 to around 1,800 in 1989 (see figure 1). These requests cover conferences, symposiums, workshops, seminars, professional association meetings, academic training, research, exhibits, or tours of industrial or government laboratories. We expect this trend to continue at least into the early 1990s.

The Target

The US scientific community is viewed by the Soviet intelligence services as a bonanza for scientific and technical intelligence. Through the USSR Academy of Sciences (see figure 2), the Soviets have implemented worldwide programs to identify, exploit, and recruit US scientific and technical people whose expertise could advance, in particular, Soviet military and weapons research and development. The Soviet intelligence services have identified areas of particular interest: physics—plasma, nuclear, light, and sound; missile, space, and aircraft technology; energetics; automated production; chemistry; new metals and materials; medicine; and biology.

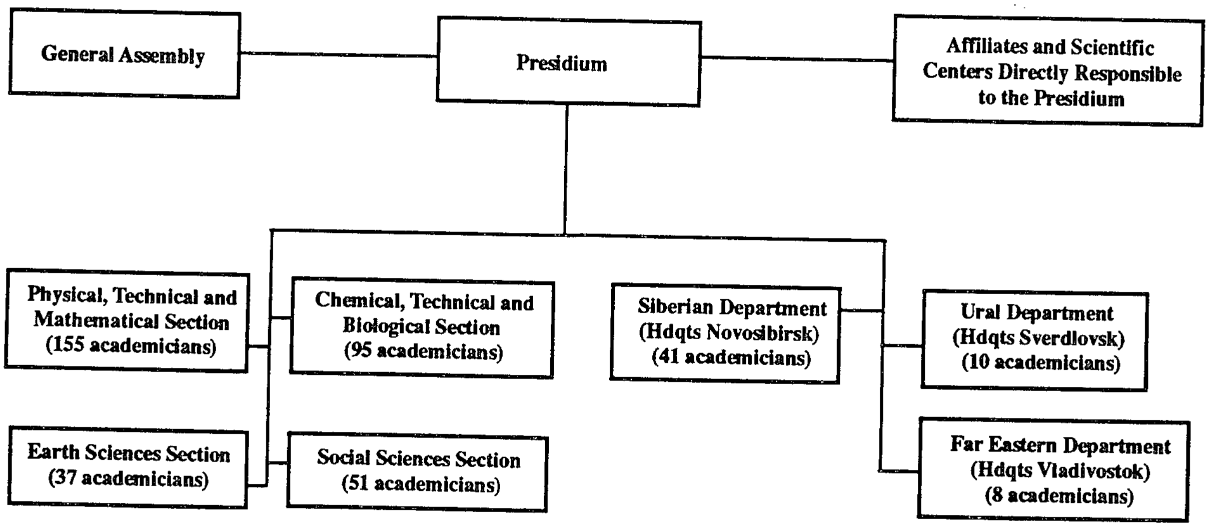
Figure 1
Soviet Scientists Requesting Visas To Visit the United States, 1984-89



325445 4-90

The United States is perceived as an ideal place for scientific and technical collection because of two essentials: data are widely available, and scientists working on classified projects are accessible. Frequently, US research facilities are involved in both classified and unclassified activities. In conjunction with unclassified work, many foreign nationals—including Soviet and East European scientists—visit a

Figure 2
USSR Academy of Sciences


General Assembly
Presidium
Affiliates and Scientific Centers Directly Responsible to the Presidium
Physical, Technical and Mathematical Section (155 academicians)
Chemical, Technical and Biological Section (95 academicians)
Siberian Department (Hdqts Novosibirsk) (41 academicians)
Ural Department (Hdqts Sverdlovsk) (10 academicians)
Earth Sciences Section (37 academicians)
Social Sciences Section (51 academicians)
Far Eastern Department (Hdqts Vladivostok) (8 academicians)

Unclassified

325446 3-90

variety of US facilities, including such sensitive Department of Energy nuclear weapons facilities as Lawrence Livermore Laboratory, California, and Los Alamos National Laboratory and Sandia National Laboratories, New Mexico.

American scientists are considered relatively easy targets. The Soviets have identified characteristics they believe make US scientists vulnerable:

- Sociability, even with casual contacts. Americans want to be liked and work at being friendly. They talk just to keep a conversation going.
- Liberal politics. They think governments may differ but people are people. Scientists are often antiestablishment and see it as fashionable to rebel. The Soviets promote the idea that science has no national boundaries.
- Egoism. They feel smarter than most people. They are susceptible to flattery, especially from fellow scientists.
- Materialism. Money and belongings are viewed as a measure of success and status.
- Careerism. They compromise integrity for professional recognition, honors, and power.

The Collector

Soviet scientists have long been used to collect information on Western weapons systems and scientific research including during World War II, when scientific delegations were sent to the West to study emerging technologies. This policy has historical precedence dating to Peter the Great, who first recognized the value of Western technology for Russian military and economic development. Oleg Penkovskiy, a GRU colonel who gave invaluable assistance to the United States in the early 1960s, reported that in 1961 he headed a group of Soviet scientific researchers sent to France "to get acquainted with some French enterprises and to maintain contacts." He was told to recruit "two or three people from among French scientific research specialists" presumably with the help of Soviet scientists.

By the mid-1960s the KGB and GRU had come to recognize the potential value of Soviet scientists as long-term collectors. Scientific and technical intelligence collection against the West, principally against the United States increasingly relied on foreign travel by Soviet specialists and contacts with foreign specialists visiting the USSR.

Apparently most Soviet scientists have been willing to collect scientific data, publications, and materials as well as agent evaluation information. We believe the reasons are materialistic, professional, and patriotic. For his cooperation a Soviet scientist receives financial compensation, some in the form of hard currency.

Beyond such immediate compensation, other incentives are probably more effective. These include:

- Travel. Good collectors have been rewarded with travel to the West. An emigre who worked at the Academy of Sciences as late as 1988 stated that "travel was usually implicitly, if not explicitly, contingent upon cooperation."

- Advancement. The case officer can help a scientist obtain a promotion or a better job. A phone call to a higher ranking intelligence service agent/co-optee in the scientist's organization is often all that is required.

Profile of a Soviet Scientist Collector

- *Travels regularly to the West*
- *Corresponds regularly with Western scientists*
- *Has funds for gifts and entertainment*
- *Can extend invitations to visit USSR*
- *Advances faster than his contemporaries*
- *Lives better than his Soviet peers*

- Western goods. US computers, software, printers, tape recorders, clothes, and other luxuries are often brought back to the USSR and sold. One emigre reported that he could sell a Western computer through his local cooperative and after paying the commissions make a profit equal to over two years' pay.

- Professional recognition. It is career enhancing to attend foreign professional meetings, publish in domestic and foreign journals, or attract well-known Western scientists to the USSR. A former member of the Academy of Sciences, stated that the ability to publish articles in a Soviet scientific journal and the "prestige and status, both inside and outside the purely academic community" conveyed by the publication of such scientific papers, was a major benefit of KGB approved foreign travel.

- Knowledge. Travel to the West gives the Soviet scientist an opportunity to collect data to advance his own research.

- Patriotism. The scientist often feels it is his duty as a Soviet citizen to advance Soviet scientific knowledge.

The Role of Intelligence Elements in the Academy of Sciences

All activities in which Soviet scientists might have contact with their non-Soviet counterparts have been filtered through specialized elements attached to the

The USSR Academy of Sciences

The USSR Academy of Sciences, which is the successor to the Russian Academy of Science founded by Czar Peter the Great in 1725, has become the most prestigious scientific organization in the USSR. Through its more than 250 institutes, the Academy today conducts research for the development of Soviet science, technology, and the national economy. Membership in the Academy is the ultimate honor for a Soviet scientist.

The Academy's General Assembly decides basic organizational issues and establishes policy. It comprises more than 300 full members and 600 corresponding members, and meets at least twice a year. New members are elected every two years at the General Assembly meeting.

The Presidium, which runs the Academy between General Assembly meetings, reports directly to the Council of Ministers and the Politburo. It is headed by the President of the Academy who is elected by the academicians and approved by the Politburo. The other 38 members of the Presidium include the Academy's vice president, its chief scientific secretary, the department heads, and a number of prominent scientists elected by the membership.

Academy's Presidium that are staffed primarily by active and retired KGB and GRU officers (see figure 3). This intelligence function has been largely centered in the Department of Scientific Cooperation with Capitalist and Developing Countries and with International Scientific Organizations—commonly called the Foreign Relations Department. That department:

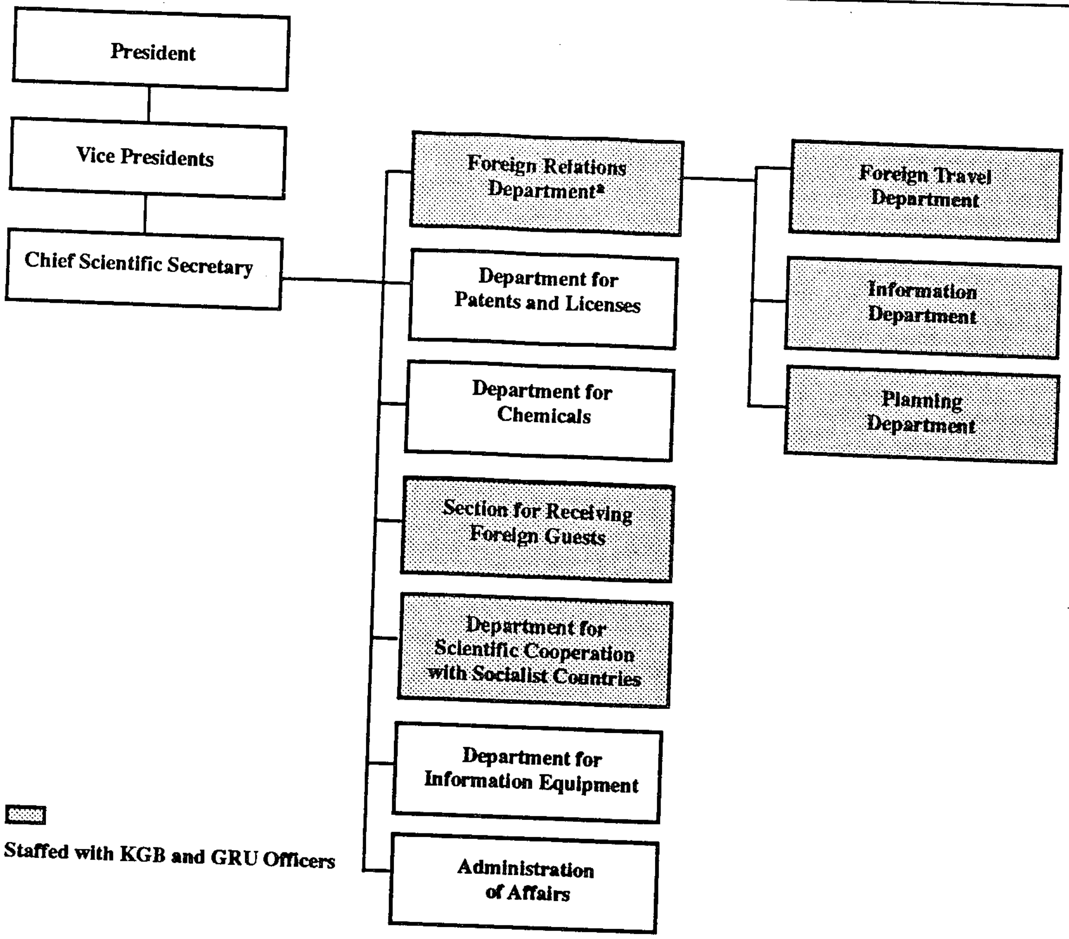
- Evaluates and recruits Soviet scientists into the collection program.
- Expedites travel requests of agents and prospective recruits.
- Gives collection guidance and leads—including names of foreign laboratories, companies, and counterparts.
- Furnishes funds for entertainment of, and gifts to, counterparts.
- Debriefs Soviet scientists on their return.
- Reports on each Soviet scientist's effectiveness as a collector.
- Assesses and recruits foreign scientists with the assistance of Soviet scientists who participate in the program.

Three departments in the Foreign Relations Department are responsible for specific parts of this overall intelligence collection charter. The **Foreign Travel Department** deals with the paperwork from scientists who wish to travel outside the USSR. The scientists submit a formal request to the Academy, and the names are cross-checked against a list of approved travelers. If the scientist's name is on the list, travel is endorsed by the sponsoring intelligence service and forwarded to the Departure Commission of the Central Committee for final approval. This process usually takes 30 to 60 days. A scientist whose name is not on the list is not automatically barred from travel but has to submit far more detailed personal information and travel justification than is required for agent/co-optees, and those being vetted for recruitment.

A second department—the **Information Department**—is devoted to intelligence tasking of traveling scientists who are not agents/co-optees. Before departure, each is told how the Academy would benefit from the trip and is encouraged to cooperate. Specific overt collection requirements may be given. Upon returning to the Soviet Union, the traveler submits a written report to this department.

The **Planning Department** prepares an annual plan for the Academy's intelligence gathering. This document matches intelligence requirements to the foreign travel proposed by each of the Academy's institutes. The objective is to maximize the intelligence gain by (1) assessing the likelihood that the foreign travel will fulfill collection requirements, (2) ensuring that the best qualified agent/co-optees are dispatched, and (3) preventing duplication of travel. Once approved by the Academy, the plan is forwarded to the State Committee for Science and Technology for final approval and funding.

Figure 3
Presidium of the USSR Academy of Sciences


President
Vice Presidents
Chief Scientific Secretary
Foreign Relations Department[a]
Department for Patents and Licenses
Department for Chemicals
Section for Receiving Foreign Guests
Department for Scientific Cooperation with Socialist Countries
Department for Information Equipment
Administration of Affairs
Foreign Travel Department
Information Department
Planning Department
▨
Staffed with KGB and GRU Officers

[a] Official name is Department of Scientific Co-operation with Capitalistic and Developing Countries and with International Scientific Organizations.

325447 3-90

The counterpart of the Foreign Relations Department, the **Department for Scientific Cooperation with Socialist Countries**, is much smaller but performs the same functions for Soviet scientists traveling to other Communist states.

The **Section for Receiving Foreign Guests**, a separate unit, is responsible for all arrangements involving scientific cooperation between the Academy's institutes and foreign scientists who are visiting the USSR, as well as representatives from foreign scientific or technical firms. More important visitors are escorted by members of the Presidium; others by a staff member of this section.

Recruiting the Soviet Scientist

A primary duty of KGB and GRU personnel assigned to the Academy of Sciences is spotting, assessing, and recruiting Soviet scientists working at institutions associated with the Academy. It also is their responsibility to provide the guidance needed to transform a raw recruit into an effective intelligence collector. In evaluating a prospective agent/co-optee, the intelligence services look for individuals with:

- Access to Western scientists who have information of strategic military intelligence value.
- A high degree of reliability. A prospective agent/co-optee is investigated to assess his loyalty.
- The capability to carry out intelligence tasks, particularly to make contacts, cultivate foreign sources, and report reliably.

During the early 1980s the vast majority of the Soviet scientists traveling abroad were reportedly cooperating to varying degrees. Most were not recruited but accepted collection requirements. In addition, a total of 370 were either agent/co-optees or considered potential recruits. A good collector's future travel requests would usually meet with little resistance. Only about 20 percent of the Soviet scientists who were allowed to travel abroad were not affiliated in any way with the collection program; travel for them derived instead from their academic standing or political connections.

Briefing

Through 1989 before traveling, most Soviet scientists were briefed and tasked with collection requirements. A scientist not affiliated with the intelligence services before departure reported to the Foreign Travel Department at the Academy. An Academy official—an intelligence officer—gave him a travel briefing. It usually included a general area orientation and a lecture on appropriate behavior. Travel funds and documentation were usually provided at this time. He also was given collection requirements in his area or a related area of expertise. For example, one computer scientist with the Academy of Sciences was given *general* requirements. That is, he was tasked with

Vetting

The Soviet intelligence services view all prospective Soviet scientists agent/co-optees as long-term assets, taking particular care in vetting and training them. The process usually lasts at least a year and goes through several distinct stages:

- *The case officer will arrange several meetings evaluating the Soviet scientist. If the prospect is bright, ambitious, interested in foreign travel, and cleared in the security check, the case officer will place his name on the KGB or GRU list of scientists being recruited.*
- *The case officer will then encourage the scientist to participate in a foreign scientific conference. He will be tasked to collect supplementary material, such as copies of papers delivered, biographies, and handouts. The scientist also will write a trip report evaluating the information and be debriefed on his contacts.*
- *If the Soviet scientist collects valuable intelligence or cultivates foreign scientists, he will be sent out again. This time he will focus on specific strategic military intelligence or specific scientists.*
- *When the scientist has shown an ability to obtain valuable intelligence and documents and that he is unlikely to defect, he will be asked formally to cooperate.*

obtaining information on Western scientists and on the status of research in the West. When he returned he was required to submit in writing: scientific information obtained, names and biographic data on contacts, an evaluation of lectures, and details on all approaches by foreigners. He was also tasked with buying commercially available Western software.

Scientists affiliated with the intelligence services got the same general area orientation briefing but also got *specific* collection requirements—people to contact, questions to ask, and/or data to obtain—from their case officers. They also received intelligence service funds for entertainment, gifts for counterparts, and for special publications or commercially available equipment.

Debriefing

Through 1989 all affiliated Soviet scientists were debriefed by their case officers after each trip. The case officer forwarded all materials to his service headquarters. The material reached the Military Industrial Commission if it responded to any of the requirements levied on the intelligence services. The case officer prepared an operational report on the scientist's effectiveness and forwarded operational leads to his headquarters. Through a second channel the scientist reported to his institute on the substantive scientific and technical gains obtained. This report was also sent to the Information Department of the Academy of Sciences.

Nonaffiliated scientists reported in writing to their local institute which, in turn, forwarded a copy to the Academy of Sciences. According to a Soviet scientist, foreign travel was not considered complete until a trip report was filed. Another scientist stated that all scientists returning from the West were required to submit a travel report including names of persons contacted, subjects discussed, where information was stored, and who had access to this information. This report was submitted to the scientists' institute, which in turn, sent it to the USSR Academy of Sciences.

Requirements

Collection requirements are developed by the Military Industrial Commission (VPK) and the State Committee for Science and Technology (GKNT) (see figure 4). The VPK is the most powerful organization in the defense-industrial establishment, comprising the top executives of the key defense manufacturing ministries. Requests from these ministries for Western documentation and unique hardware are the bases for requirements. Once approved by the VPK, requirements are levied on the KGB, the GRU, and other national-level collection agencies.

Major Collection Targets

The number of US academic centers targeted by the Soviet intelligence services increased from about 20 in the late 1970s to over 60 in the early 1980s. These academic institutions were cited in VPK collection directives as sources of both applied military-related technology and civilian scientific data. Collection through the Academy of Sciences against scientific conferences and US academic centers, and defense contractors, also has been productive.

Scientific Conferences

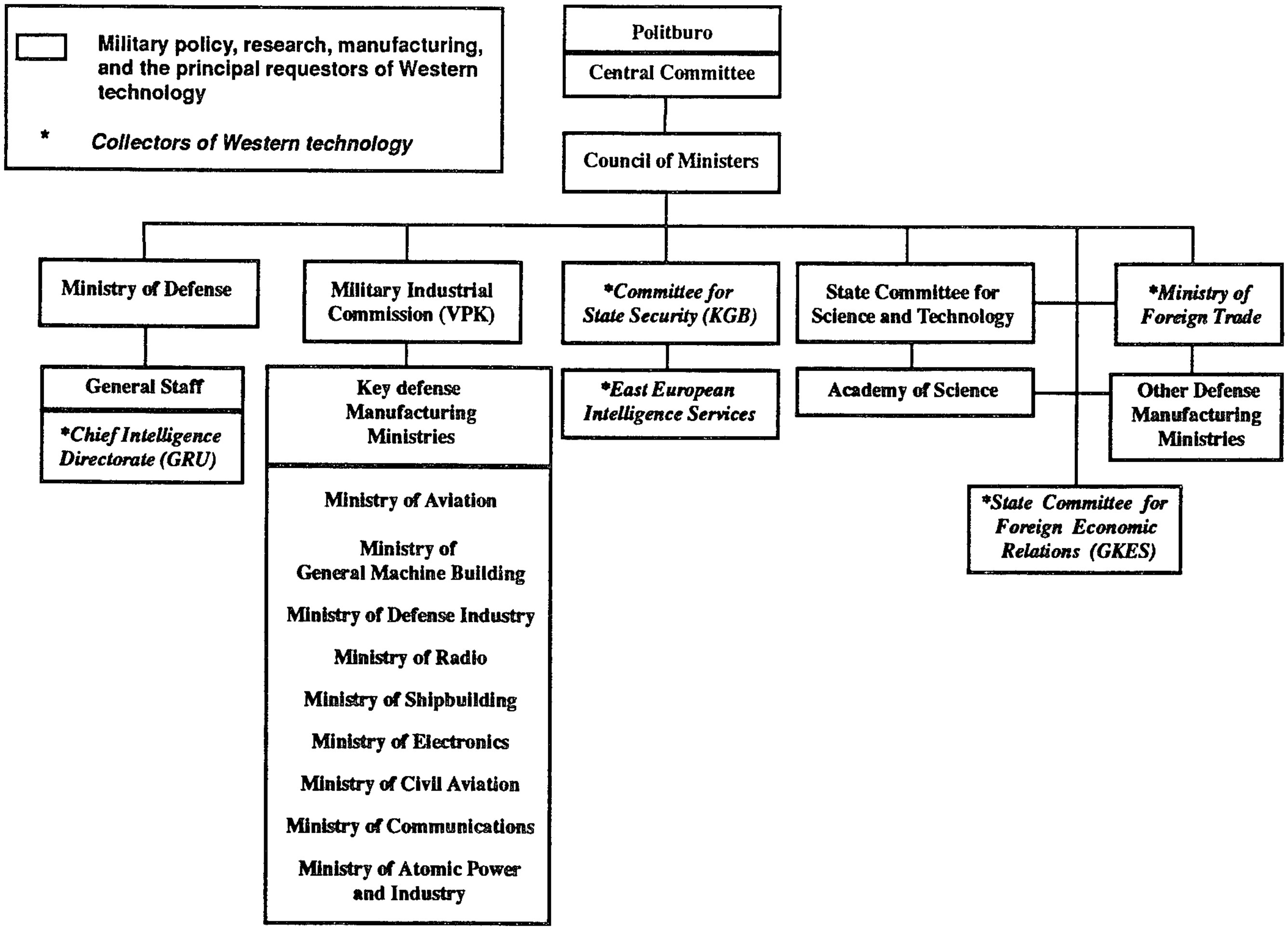
Information collected from professional and academic conferences on applied science and technology has helped Soviet defense efforts. For example, in the late 1970s at least 35 conferences worldwide were identified by the VPK program as potential sources of solutions to military research problems.[1] These included conferences on materials, missiles, engines, lasers, computers, marine technology, space, microelectronics, chemical engineering, radars, armaments, and optical communications. The Soviets judged some of the data from these conferences to be among the most significant contributions to their military projects. Their attendance at the:

- International Radar Conference helped improve circuit designs for synthetic aperture satellite radars and aircraft over-the-horizon radars.

- Conference on Integrated Optics helped identify ways to produce a qualitatively new category of integrated optical devices for fiber-optics communications.

[1] For additional data on Soviet collection activities at scientific conferences and universities as well as acquisition of Western military technology see *Soviet Acquisition of Militarily Significant Western Technology: An Update, 1985.*

Figure 4
Key Organizations Involved in Managing Military Research and Manufacturing and the Acquisition of Western Technology


□ Military policy, research, manufacturing, and the principal requestors of Western technology
* Collectors of Western technology
Politburo
Central Committee
Council of Ministers
Ministry of Defense
Military Industrial Commission (VPK)
*Committee for State Security (KGB)
State Committee for Science and Technology
*Ministry of Foreign Trade
General Staff
*Chief Intelligence Directorate (GRU)
Key defense Manufacturing Ministries
Ministry of Aviation
Ministry of General Machine Building
Ministry of Defense Industry
Ministry of Radio
Ministry of Shipbuilding
Ministry of Electronics
Ministry of Civil Aviation
Ministry of Communications
Ministry of Atomic Power and Industry
*East European Intelligence Services
Academy of Science
Other Defense Manufacturing Ministries
*State Committee for Foreign Economic Relations (GKES)

The Soviet program to acquire militarily significant Western technology is a success story. Over 3,500 specific collection requirements for hardware and documents were satisfied for the industrial ministries for just the 10th Five-Year Plan (1976-80). About 50 percent of more than 30,000 pieces of Western one-of-a-kind military and dual-use hardware and about 20 percent of over 400,000 technical documents collected worldwide in response to these requirements were used to improve the technical performance of very large numbers of Soviet military equipment and weapon systems. According to the Soviets, about one-third of the VPK requirements are totally or partially fulfilled annually. In fact, each year the number of VPK requirements grows by about 15 percent. This is a strong indication that the expanding Soviet military industrial program continues to rely on Western technical solutions and advances. It also indicates increased collection success and user expectation.

325448 3-90

- Conference of the Aerospace and Electronic Systems Society of the Institute of Electrical and Electronics Engineers produced technical solutions to problems associated with low-altitude target detection radars.

- International Conference on Radar helped develop signal processing for passive jamming suppression methods and for radars to detect distant aircraft targets.

- International Conference on Nontraditional Energy Transformation Systems refined directions of research on space-based nuclear reactors.

- Conference on Millimetric and Submillimetric Equipment produced design solutions for millimeter wave proximity fuzes.

- Symposium on Solar Energy Conversion increased efficiency and decreased costs for electron beam deposition of coatings on solar components for space vehicles.

According to Soviet estimates, these conferences alone, particularly the first three, produced savings of millions of rubles in long-range military research projects. These professional and scientific conferences remain specific VPK targets.

Recruiting US Scientists

Soviet scientists have helped the Soviet intelligence services with recruitment. Soviet scientists often have been tasked to:

- Collect biographic and assessment data on foreign scientists. Soviet scientists are encouraged to visit and correspond with foreign counterparts. Some relationships date back over 20 years.
- Evaluate foreign scientists' professional capabilities.
- Aid in evaluating Western scientists' personal vulnerabilities and assessing receptivity to recruitment.
- Invite selected foreign scientists to the USSR to allow intelligence officers to observe them under controlled conditions, and, in selected cases, to place foreign scientists in compromising positions.

Other Academic Related Collection

During the late 1970s and early 1980s, Soviet scientific collection directives targeted some of the finest universities in the United States. Carnegie-Mellon, MIT, Cincinnati, Kentucky, Michigan, and Wisconsin (as well as defense contractors) were identified as sources for information on new high-strength, high-temperature alloys such as titanium; on lightweight structural alloys; and on powder metal processing. California Institute of Technology, Harvard, and MIT were targeted for their work in space, aviation, and missile systems. California Institute of Technology and MIT were also cited as sources for transonic, supersonic, and hypersonic aerodynamic research, as were the Polytechnic Institute of New York, Princeton, and Stanford. Kansas, MIT, Ohio State, and Penn State were identified for electrohydraulic control systems applicable to aircraft, helicopters, and the Soviet version of the US space shuttle. Research applicable to future high-energy laser and particle beam weapons was sought from MIT, Denver, and Princeton.

A few Western scientists have reported recruitment pitches or attempts to compromise them while in the USSR. They had been invited by the Academy to attend conferences or visit scientific facilities. Typically, they were met by a longtime friend from the Soviet scientific community who introduced them to a pleasant man described as an associate. They attended several social functions with this Soviet who also escorted them on local tours. The scientists said that the Soviet sounded them out on their willingness to provide either classified or proprietary data. In each reported case the US scientists expressed indignation, and the subject was dropped. The Soviet never appeared again. Others have reported attempts to compromise them including approaches by Soviet women at social functions and in hotel rooms, as well as offers to sell such things as antiques.

The Computer Age

The advent of computer networks linking scientists and their research institutions vastly complicates any effort to identify Soviet scientific espionage. For example, foreign travel may become less important, as computers become more directly interconnected, allowing scientists anywhere in the world to talk to each other—and, in some cases to access information in data bases at Western academic and defense-related institutions.

This capability has been available for some time, but in 1989 the USSR took an important step toward increasing the breadth and availability of access, by applying (with Poland, Czechoslovakia, Hungary, and Bulgaria) to be connected to the European Academic Research Network (EARN). Approval of the application in April 1990 provided Soviet and East European users access far beyond simply a link to computers throughout Western Europe. Through EARN, the Soviets would be connected to Internet, a US network serving defense, research, and academic organizations worldwide.

A number of threats are inherent in the trend toward computer linkage. The most obvious is the increased ease with which a Soviet can discuss professional matters with Westerners working on similar projects. A user also can put out a blanket request for information on any subject, and it may not always be obvious that the requestor is working for the USSR. In addition, the Soviet Academy of Sciences can use a computer network to issue general invitations to conferences—in hopes that the responses will identify untapped research institutions or individual scientists that later can be targeted for specific information.

Access to data in the computers connected to a network normally is controlled, so that specific files can be read only by authorized users. However, the Soviets have demonstrated that an innovative "hacker" connected to computers containing sensitive information can evade the access controls in order to read that information. In the "Hanover Hacker" Case, for example, the Soviet intelligence services used West German computer experts to access US restricted data bases, obtaining both software and defense-related information.

Soviet scientists also have been used on occasion to introduce an intelligence officer to a foreign scientist while outside the USSR. Again in such cases the Soviet scientists would not be present for the pitch. Lastly the Soviet scientist himself can be used to pitch the foreign scientist. Direct involvement of Soviet scientists in recruitment at home or abroad is rare because of the risk to the credibility of the Soviet scientist and the Academy as well as the possibility of compromising a successful collection program.

Effectiveness of the Program

By using scientists as collectors, the Soviets have increased their chances of fulfilling outstanding scientific and technical collection requirements. Scientists not only have unique access to both published and unpublished material through US counterparts, but they are discriminating collectors who are likely to know what is valuable.

In addition, the program has provided unique opportunities to:

- Access scientific laboratories and other scientific and technical facilities. Visa data indicate that Soviet scientists attending scientific conferences in the United States will attempt to schedule visits to related facilities. For example, a Soviet nuclear physicist attending a three-day conference in San

Francisco asked to visit US counterparts at San Francisco State University and UC Berkeley as well as to tour Lawrence Livermore Laboratory.

- Collect biographic data on specific scientists, their families, friends, colleagues, as well as data on the status of their programs.

- Arrange meetings between Soviet intelligence officers and US scientists who appear vulnerable to recruitment.

- Obtain samples of embargoed hardware. One Soviet scientist was reported to have obtained a specific type of fiber-optic cable from a foreign scientist. By duplicating the cable's elastic coating, the Soviets improved the flexibility of their fiber-optic cable twentyfold.

This collection system appears relatively inexpensive and risk free:

- The host country pays most travel expenses.
- Recruiting, training, and management costs are relatively low.
- There is little risk of exposure because recruitment attempts can be made in the USSR or a third country after extensive evaluations, and the Soviet scientist generally is not present for the pitch.
- Risk of defection is no greater than in other programs.

The program functions on two levels. It fulfills national scientific and technical collection requirements. Equally important, it often directly helps the Soviet scientist's own work. This effect can be immediate and dramatic, saving time and money and advancing careers. This added incentive ensures highly motivated and cooperative collectors.

Implications

The net impact of Gorbachev's reforms on Soviet intelligence targeting of the US scientific community is unclear. The country's growing economic distress and Gorbachev's commitment to technological modernization may make S&T intelligence an even higher collection priority than in the past. The evidence indicates that Soviet intelligence activity in this area continues unabated. It seems likely, however, that over time a desire to improve relations with the West and to seek economic assistance may cause the Soviet intelligence services modus vivendi to become more cautious, more inclined to avoid high-risk operations whose exposure would embarrass Gorbachev, and tarnish the country's new international image. This would place increasing importance on the use of Soviet scientists as collectors because of the low risk aspects of this collection program. In addition, the end of the Cold War is undoubtedly eroding US scientists' suspicions of Soviet motives and providing the USSR with greater access, thereby increasing US vulnerabilities.

Many Soviet scientists are likely to become more reluctant than in the past to cooperate with the Soviet intelligence services collection efforts. KGB leverage over them has decreased as opportunities for professional travel have expanded and become less dependent on KGB vetting for political reliability.

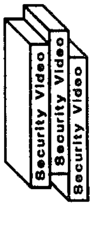
A Clearinghouse for Security Education Products

A couple of Bulletins ago we ran the following announcement and got a good response. We're running it again in case we missed you the first time.

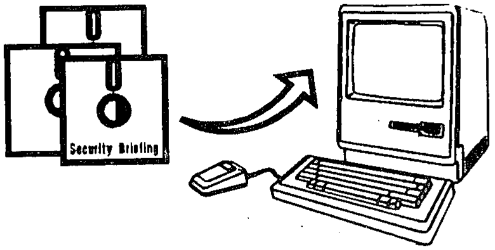
When it's time for you to give a security briefing, does the availability of training materials remind you of Mother Hubbard's cupboard? When presenting security briefings, have you ever felt that you and the flight attendant addressing a plane full of frequent flyers have a lot in common? Whether you are a security novice and know no sources for security education materials or a security expert but know only the same old sources, a Security Education Project is underway in an effort to help.

The Joint Industry/Government Security Awareness Group (JIGSAG) is supporting the Department of Defense Security Institute's efforts in setting up a clearinghouse for security education materials. The idea is to have a central point to send products that have proven themselves effective—in other words, that your audience likes—so that, with everyone sharing products, you suddenly have a tremendous pool of resources to draw from.

The products initially targeted for collection are *videotapes* and *PC-based tutorials/briefings*. The members of the Project encourage your participation and ask that you forward your product to:



Del Carrell
DoD Security Institute
8000 Jefferson Davis Hwy
Bldg 33E
Richmond, VA 23297-5091
(804) 279-5314, DSN 695-5314
fax (804) 279-6406

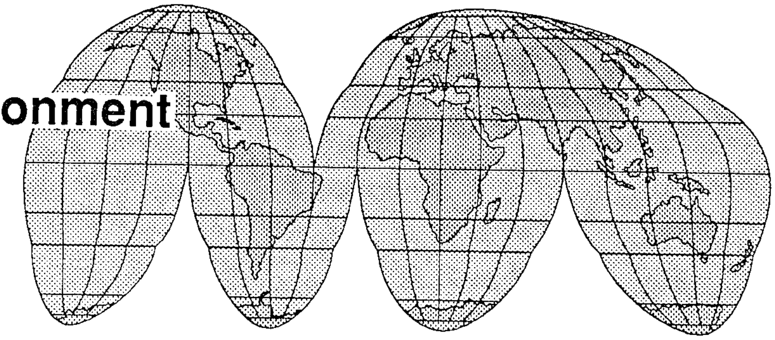


All products will be evaluated by JIGSAG for accuracy, quality, propriety in accordance with defined standards, and applicability within the DOD/Industrial Security communities. The committee will also send a description of *every* product to the DODSI along with the evaluation results. An example is provided on the next page. DODSI will have the best ones reproduced and distributed either through the DIS Education and Training Specialists (for loan) or through inexpensive commercial distribution centers (for purchase—$20-30). DODSI will also publish a catalog of *all* submitted training materials, similar to what is provided in its "Training Aids for Security Education."

Don't be reticent. Even if your video hasn't won an Oscar, it's a "go" for entry in the catalog and may be a good candidate for distribution. Why don't you take a minute to rummage through your cabinets for any training products you've put together. They don't have to be stellar acts—their novelty and availability are important factors, too.

With your help, this could turn out to be a great success!

The New Global Environment in Defense Industry



by William B. Bader

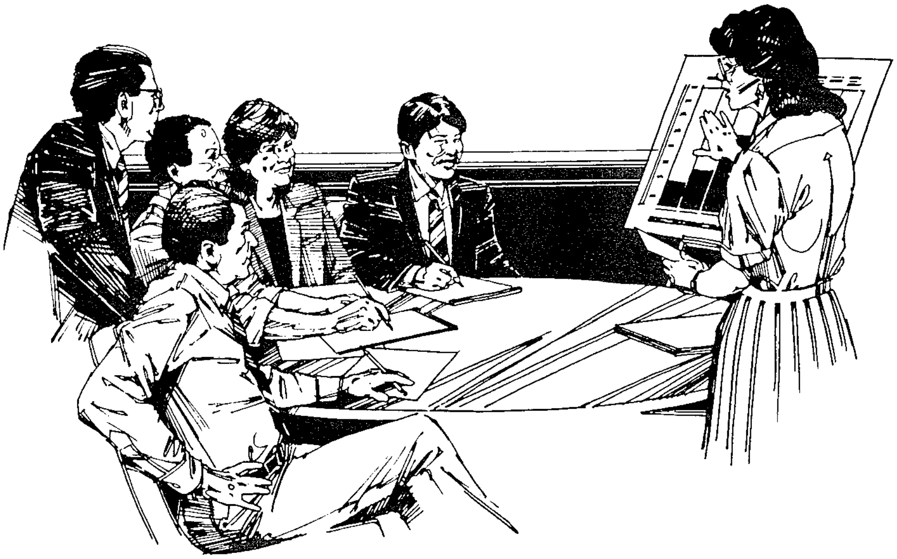
The following address by Dr. William Bader, senior vice-president of SRI International's Policy Division, was given to the recent symposium on security awareness in Monterey California. In his personal account, Dr. Bader discussed technological and societal trends that will define a new environment for defense industry in the 1990s—one in which security issues will be extremely important. He argues that in the new multi-national environment, the control of technology crucial to national interest will depend on a greater sense of ethics, personal responsibility, and mutual education about what information can be shared what can't.

A new generation of scientists, engineers, and management consultants will create the new security consciousness in the course of their daily work. Every laboratory, cubicle, and office that contains networked or modemed computer equipment will be an experiment in security awareness. And SRI is a particularly interesting place for that kind of experiment. With an organization that has about 2,600 scientists, engineers, social scientists, and management consultants, it features some rather remarkable diversity. The population can be characterized on a spectrum that ranges from a high level of security awareness to a low one.

A large segment of our employee population has a high level of security awareness. That segment consists of the engineers who are part of the cleared (to perform classified government work) community in every sense of the word. They work in many very major classified programs. At the other end of the spectrum is a new group. The new group tends to be multinational, ethnically diverse individuals with few ties to the United States except in their work pattern. This group is similar to the increasing number of management consultants and people who work with big international firms that have become more global and more multinational in their activities and scope.

Probably a quarter to half the people who work with me (this number excludes people cleared for classified work) would find the rhetoric, if not the content, of this meeting somewhere between ludicrous and amusing because it doesn't fit with the world as they see it, and it doesn't fit with the experience they've had. One of the major challenges we face in increasing security awareness is in the refinement of the rhetoric and in the development of a dialogue with these new practitioners.

Let me just say a few things quickly about that environment as I see it because how we all address what needs to be done and how we think about these issues is important. Let me first mention something about my own background. I formed the way I perceive the world, and how I perceive security issues and security awareness, as a LTJG in Japan in the 1950s and also as a CIA officer in the 1960s. As I look back on it, nostalgically, the environment was remarkably predictable and manageable—something we really don't have today.



Today, we're dealing in an arena in which sovereign nations compete to gain advantage in ways other than the traditional means of international trade. Today large corporations operate as world players and that serious difference creates a problem. Fifty of the global corporations we track at SRI have 40% of their sales outside their home countries. Xerox reports that 50% of its employees and 50% of its sales are outside the United States. Of Philips's assets, 60% are in Europe, 30% in North America and South America, 10% in Asia and Pacific. IBM employs 40% of its employees outside the United States. Whirlpool employs 43,000 people in 45 countries. What we're really doing now is competing in an increasingly borderless business world in which a company's national identity may be really difficult to define. The ambiguity creates enormous problems for us concerning the national identities of company X or company Y.

Of course, at the same time, governments are opening their borders to participate in these global economics. As you probably all know, foreign investment now has increasingly overshadowed trade flows. Foreign exchange transactions are running on a daily basis between $325 billion and $375 billion, while trade volume is some $70 billion. You can see there's a big difference. So what does it mean?

It means that foreign direct investment all around the world has been growing at the rate of about 20% annually—four times faster than trade. Foreign direct investment is reshaping the whole international business structure. For example, the Japanese FDI (or foreign direct investment) in the United States has dramatically altered the structures of the U.S. automobile industry, machine tool industry, and the financial service industries. From the skyline of Los Angeles to the Rockefeller Center in New York, there are many indications of substantial investment by the Japanese, including what the Japanese may or may not do to the U.S. entertainment industry. What are the implications of this foreign direct investment throughout the world and, most particularly, of the foreign investment in the Unites States? We have to begin to wonder whether the nation-state is, in fact, economically and competitively the relevant unit of analysis.

How about your world here, which is often associated with the defense industry? The defense industry is becoming smaller, more consolidated, and more global in nature. Players will seek international affiliations, which we're now seeing, let's say, between General Dynamics and Mitsubishi. We'll eventually see a few large, major diversified, and very, very global firms in the United States, France, Germany, the United Kingdom, and Japan. These firms will be the survivors of what is very obviously going to be a shakeout in the defense industry. It will have very strong implications for all of us, and particularly for you. A dramatic increase in international partnerships and consortia is going to take place. Some of them are particularly noteworthy and I think worrisome because they have implications for information flow, information management, and competitive advantage. I'll just name a few. Lockheed and Aero-Spatiale, General Dynamics and British Aerospace, the U.S.-French CFM International, which is General Electric and SNECMA; the French Aircraft Engine Manufacture; and McDonnel Douglas and Samson. Others involve non-U.S. companies and have some of the same worrisome implications. The consolidation between Daimler-Benz and Mitsubishi has a truly haunting antecedent in the axis alliance of World War II.

All this comes at a time in the world when the U.S. defense industry moves into the 1990s with many more problems than those brought by smaller defense budgets. Just one note for the defense industry world: The percent of debt to equity among the 10 defense companies in the S&P Aerospace Index has more than doubled in the past seven years. The U.S. defense industry at this stage is becoming hungry for foreign alliances and investment. Defense companies are exceedingly vulnerable to the temptation to traffic in information and in data—and not necessarily the information and data of the 1950s, but the essential information and data in today's world that defines whether we are going to be, as a nation-state, competitive in this market place.

The next factor I'd like to discuss is sociological in nature. The process and product of security awareness programs in the Defense Department and the defense industries will become much more complicated and ambiguous because of the presence of foreign nationals in our facilities. Foreign nationals will become more common not only in our facilities, but in our laboratories, at our dinner tables, and increasingly in our bedrooms. Statistics indicate that the population at U.S. universities and graduate schools is increasingly foreign. At some graduate schools in the United States 60-65% of the graduate students in physics and in engineering come from another country. These people will be coming into our industries, including our defense industry.

And what does that mean? At a place like SRI we have a mixed population. You go into one laboratory and you find a Czech. In the next laboratory the scientist you find is Chinese. The situation generates a real problem of managing these constituencies within the new environments we're creating. We have situations now at SRI where the poor chaps over in the cleared community receive notices that you may not go to the dining room for the next 2 1/2 days because of visiting Czechs or Chinese. The demographics are changing in our world, and the security world has to adjust.

Now let me turn to the implications of all this and to some of the recommendations inspired by our examination of national economics, strategic alliances, and cultural and national diversity. But first, I think we ought to acknowledge that whatever the demographic, economic, and competitive changes have wrought, a more important factor is at work. Information, data, and analysis are—and will remain—the most powerful engines and tools of economic security and power. The management of these precious resources is our biggest task. I think when we're trying to understand this environment and operate within it, we must keep our eye on information, data and analysis: their use, their traffic, and their essential nature to the competitive edge.

I think we ought to acknowledge at the same time that enhanced security awareness in the 1990s will be the result of a partnership, discussion, and interaction at all levels: in corporations and businesses. Our efforts will be fruitless if they depend on administrative, legislative, statutory fiat. Partnership and discussion within your company is the trend, and it has to be the trend. No other way will work. At a time of constrained resources for security programs and for security education, we should take advantage of that reality. And I think that we are going to have to see more voluntary and more proactive involvement at all levels of your organizations.

We must make an attempt to educate and to convince people that some new words are relevant and important in this process. Let me give you one that you might think is absolutely heretical in the world that we now live in. The word is *ethics*. I believe that in the 1990s the true enemies of this state in terms of our economic and national security will be the Boeskys and the Millikens of the world rather than the Walkers. Individuals who are prepared to traffic in information and inside knowledge, whether they have to do with technologies or market trading, are a threat to our nation in a way that is much less obvious than the traditional security risk. No ethics and no standards existed among the major operators in what is now known as the Decade of Greed: the 1980s. In the security world, we need to work for ethics and ethical standards: personal standards, professional standards. We need to understand competitive advantage, to understand that you can damage the security of the United States or the economic security of the United States if you make deals, if you pass technology—if you do things that are damaging in an ethical sense.

I think these are the major forces, and I hope that you take away from these proceedings the desire to implement these kinds of attitudes and approaches in your own organizations. I'm not saying that you shouldn't have procedures and rules. I am saying that a more basic dimension is important.

Anyone in the information industry these days faces tough decisions. One of my programs at SRI takes information about emerging technologies from all over the world and creates documents called technology profiles. I have profiles of everything from advanced silicone microelectronics to biocatalysis; from fiber-optic sensors to neural networks. And what do I do with this technology information? I sell it all around the world. I sell it to businesses. I sell it to Mitsubishi. I sell it to whomever is prepared to pay for it. This is technology information. Is it a technology leak? Is it a dangerous loss of information as far as the American competitive position is concerned at this stage? In the last analysis, it is going to depend on all of us who are in this business of understanding the usefulness of data, information, and analysis to be responsible in terms of our national interest about what goes into those packages. That's where I think attitudes must change. We need more interaction. We need more mutual education. And we need a hell of a lot more sense of ethics and responsibility on the part of individuals who are dealing with information in this world.

William Bader is a former Naval officer and later served as a senior staff member of the Senate Foreign Relations Committee. He has authored a number of publications in the fields of national security, arms control, foreign affairs, and government policy.

Video at FilmComm

Jonathan Pollard – A Portrayal

Jonathan Pollard was an employee of the Navy, but because of his position as a counterintelligence analyst, he had access to hundreds of classified documents from the intelligence departments of many federal agencies – and at the time of his arrest, had stuffed enough of these documents in his apartment to fill a space 10' x 6' x 4'. Pollard is an American who spied for Israel. He is serving a life sentence for his espionage work. And the reason he is, is thanks in part to an observant co-worker who noticed suspicious activity and was smart enough to report it. This video reenacts the events at Naval Intelligence Command in Suitland, Maryland, that led to the realization Pollard was involved in more than just doing his job. Produced by the Defense Intelligence Agency, it runs for 18 minutes and is available in 1/2" or 3/4" videotape.

To order copies or for additional information write or call:

FilmComm
641 North Avenue
Glendale Heights, IL 60139
(708) 790-3300
fax: (708) 790-3325

Cost is $24.00 for prepaid and $26.00 for invoiced orders. The price include all dubbing and handling charges except postage. Mode of transportation is your choice (UPS, First Class, Federal Express, etc.). The usual postage charge is about $2.50 except, of course, for overnight and priority shipping. Other security education videos available from FilmComm include The Dark Side of Espionage, Espionage Alert, Espionage 2000, two foreign travel videos, and the Project Slammer series. Please call them for additional products and information.

Research Notes From

PERSEREC

Michigan State University: Graduate Study and the NISP

President Bush recently approved the development and implementation of a National Industrial Security Program (NISP) to provide government and industry improved industrial security protection at a lower cost. Several Michigan State University, School of Criminal Justice alumni, themselves working in government and industry, have spurred the revitalization of the industrial security graduate curriculum at Michigan State University. Course offerings now provide students with exposure to key government and industrial specialists during weekly seminars. The School of Criminal Justice is working with both alumni and government to establish the Center for Security Management and Leadership, which will extend security education beyond the classroom by providing continuing education seminars to executives.

Professor Merry Morash, the director of the school, notes that a benefit from locating the program at Michigan State University is the potential for interdisciplinary work in such fields as psychology, political science, and labor and industrial relations. Students in the graduate program are exposed to a wide range of faculty and have opportunities for interdisciplinary research. They also have access to a state of the art computer laboratory, which is dedicated to computer applications, including research, that support the NISP.

Through its Broad Agency Announcement (BAA) grant program, PERSEREC is assisting both students and faculty in the development of research topics and assistance in funding for those projects. The BAA provides financial assistance for Master's and Doctoral students as well as institutional grants for faculty members. For a copy of the announcement, dated April 1991, please write to PERSEREC at the address listed below.

PERSEREC is pleased to have been asked to assist in the implementation of this new graduate program. Graduate theses and policy papers will be part of the long-term success of the NISP. Students participating in this program include individuals on leave from industry or government, who return to the campus for a year, as well as individuals moving directly from a bachelor's degree program.

Those desiring information on the graduate program should contact Dr. Merry Morash, Director, School of Criminal Justice, Michigan State University, Baker Hall, East Lansing, MI, 48824-1118.

The Defense Personnel Security Research Center, 99 Pacific Street, Building 455, Suite E, Monterey, California, 93940-2481. PERSEREC is tasked with research which will improve the protection of our nation's security through better personnel security procedures, programs and practices.

Security Awareness Publications Available from the Institute

Publications are free. Just check the titles you want and send this form to us with your **address label**

Our address is:

DoD Security Institute
Attn: SEAT
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, VA 23297-5091
(804) 279-5314/4223 or DSN 695-5314/4223

□ **Recent Espionage Cases: Summaries and Sources**. July 1994. Eighty-five cases, 1975 through 1994. "Thumb-nail" summaries and open-source citations.

□ **Announcement of Products and Resources**. March 1996. A catalog of security education videos, publications, posters, and more you can order.

□ **DELIVER!** Easy-to-follow pamphlet on how to transmit and transport your classified materials. Written specifically for the Department of Defense employee. September 1992.

□ **Terminator VIII**. Requirements for destruction of classified materials. Written specifically for the Department of Defense employee. September 1992.

□ **STU-III Handbook for Industry**. To assist FSOs of cleared defense contractors who require the STU-III, Type 1 unit. Covers step-by-step what you need to know and do to make the STU-III a valuable addition to your facility's operations.

□ **Survival Handbook**. The basic security procedures necessary for keeping you out of trouble. Written specifically for the Department of Defense employee. April 1995.

□ **Layman's Guide to Security**. The basic security procedures that you should be aware of when handling classified materials in your work environment. May 1995.

□ **Acronyms and Abbreviations**. Twelve pages of security-related acronyms and abbreviations and basic security forms. October 1995.

□ **Take A Security Break.** Questions and answers on security and other topics.

□ **Take Another Security Break.** More questions and answers.

□ **Lock Up!** A pamphlet on the structural standards and other security requirements for the storage of conventional arms, ammunition, and explosives. August 1995.

Security Awareness Bulletin. A quarterly publication of current security countermeasures and counterintelligence developments, training aids, and education articles. Back issues available from the Institute:

□ The Case of Randy Miles Jeffries **(2-90)**
□ Beyond Compliance - Achieving Excellence in Industrial Security **(3-90)**
□ Foreign Intelligence Threat for the 1990s **(4-90)**
□ Regional Cooperation for Security Education **(1-91)**
□ AIS Security **(2-91)**
□ Economic Espionage **(1-92)**
□ OPSEC **(3-92)**
□ What is the Threat and the New Strategy? **(4-92)**
□ Acquisition Systems Protection **(1-93)**
□ Treaty Inspections and Security **(2-93)**
□ Research on Espionage **(1-94)**
□ Information Systems Security **(2-94)**
□ Acquisition Systems Protection Program **(3-94)**
□ Aldrich H. Ames Espionage Case **(4-94)**
□ Revised Self-Inspection Handbook/Summary of NISPOM Changes **(1-95)**
□ The Threat to U.S. Technology **(2-95)**
□ Entering a New Era in Security **(1-96)**